John C. Ellis, Jr.
California State Bar Number 228083
Reuben C. Cahn
California State Bar No. 255158
Federal Defenders of San Diego, Inc.
225 Broadway, Suite 900
San Diego, California 92101-5008
Telephone: (619) 234-8467
John_Ellis@fd.org/Reuben_Cahn@fd.org

Attorneys for Ms. Kissane

United States District Court

Southern District Of California

(Honorable Larry A. Burns)

United States Of America, Plaintiff, v. **Nicole Kissane (2),** Defendant.	Case No.: 15cr1928-LAB **Memorandum of Points and Authorities in Support of Defendant's Motion to Suppress Evidence**

I. Introduction And Summary Of Argument

In the course of its investigation, the government filed numerous applications to search and seize Ms. Kissane's personal property and data. First, the government received a sneak and steal warrant, allowing them to, without notice, search and seize items from Ms. Kissane's car on November 19, 2013. *See* Exhibit A. The warrant was executed on November 20, 2013. Second, the government received a warrant to search the home of Ms. Kissane's mother on December 16, 2013. Exhibit B. The warrant was executed on December 18, 2013. Third, on three occasions, the government filed applications for the installation of pen registers and trap and trace devices on two cellular phones associated with Ms. Kissane on April 9, 2014. Exhibit C (order) and Exhibit D (application and order); Exhibit E (application and order); Exhibit F (application and

order); and Exhibit G (application and order).1 The April 29th applications (Exhibits F and G) include the requirement that the service provider disclose "the location of the single primary cell site/sector (physical address) at call origination and call termination." Exhibit F, p. 2; Exhibit G, p. 2. Fourth, the government filed applications for the historic cell site location data for cellular phone numbers associated with Ms. Kissane. Exhibit H (application and order) and Exhibit I (application and order). The government filed an additional application for an order describing subscriber information on December 19, 2014. Exhibit I (application and order). Fifth, on two occasions, the government filed applications for cell tower information; requesting that various service providers to disclose all the subscriber information made from cell towers in various locations. Exhibit J and Exhibit K. Finally, the government filed an application for data associated with Ms. Kissane's email account. Exhibit L.

The various searches and seizures of Ms. Kissane's personal property and data resulted in violations ranging from the Fourth Amendment to the First Amendment. The warrants for her car and home violate the Fourth Amendment and Federal Rule of Criminal Procedure 41. The government seized and searched all the data from every digital device it found, despite lacking a showing of probable cause or a search protocol. The government searched Ms. Kissane's car and seized items therein without providing proper notice. The government seized data without a warrant and without a showing of probable cause. And government agents mislead the magistrate judges in order to get warrants. Under these circumstances, all evidence seized and derived from the above warrants and applications should be suppressed.

---

[1] On June 23, 2014, the government filed applications to extend these orders for an additional 60 days. On December 10, 2014, the government filed applications to install a pen register and trap and trace device on cellular phones associated with Ms. Kissane. Because the information contained in these applications and orders are largely duplicative, they are not included herein. In these motions, Ms. Kissane is seeking to suppress all evidence seized or derived from these applications and orders as well.

II. Suppress All Evidence Seized And Derived From The Search of the Honda Fit and Home.

There are multiple problems with the search warrants for Ms. Kissane's vehicle and for her mother's home. Because, save for one additional issue with the search of the Honda Fit, the issues are identical, they are consolidated in this motion. This court should suppress evidence from the searches because the warrants: (1) lack probable cause; (2) violate the particularity requirement; (3) are overbroad; and (4) the good faith exception does not apply. Additionally, the court should suppress evidence from the covert search of Ms. Kissane's car because the failure to timely notify her about the search and seizure of items violates the Fourth Amendment and Federal Rule of Criminal Procedure 41.

A. The Warrants Lack Probable Cause

The Fourth Amendment's Warrants Clause requires that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." Probable cause for a search requires a "fair probability that contraband or evidence of a crime will be found in a particular place," *Illinois v. Gates*, 462 U.S. 213, 238 (1983), and "probable cause must exist to seize all the items of a particular type described in the warrant." *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9th Cir. 1991) (citing *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (Kennedy, J.)). Here, the warrants neither establish that a federal offense was committed or that instrumentalities of an offense would be located in either the car or the home. Therefore, because the warrants lack probable cause, the evidence seized and derived from them should be suppressed.

B. The Warrants Are Overbroad

The Fourth Amendment requires a warrant to be limited in scope to prevent the "general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). This concept is referred to as breadth and "may be defined as the requirement that there be probable cause to seize the particular thing named in the warrant." *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 57 (9th

Cir.1991). "[P]robable cause means a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of circumstances." *United States v. Diaz*, 491 F.3d 1074, 1078 (9th Cir. 2007) (internal quotation marks omitted). Thus, the warrant "must be no broader than the probable cause on which it is based." *United States v. Weber*, 915 F.2d 1282, 1285 (9th Cir. 1990). This rule "prevents the magistrate from making a mistaken authorization to search for particular objects in the first instance, no matter how well the objects are described." *Id.* at 1285–86.

1. Overbreadth

A warrant may not be so broad as to encompass nearly everything in a location to be searched, thus effectively obviating the particularity requirement, and amounting to the general warrant dreaded by the Constitution's Framers. *See Marron v. United States*, 275 U.S. 192, 196 (1927). But that's exactly what happened here. The list of items the search warrants allowed the agents to seize effectively created general warrants allowing the seizure of nearly every item in the car and the house.

a. The November Warrant

The search warrant application for the Honda Fit provides that all "[i]tems and records constituting and containing evidence, fruits, and /or instrumentalities of violations of 18 U.S.C. §43 (force, violence, and threats involving animal enterprises)" can be seized. Exhibit A, p. 16. Separate and apart from these items, the search warrant also allows for the seizure of the following items:

1. **Any** computer systems, digital or analog videos, iPhones and other smartphones, iPods, other digital media storage and playback devices, and cell phones related to or used to commit or facilitate commission of 18 U.S.C. § 43, containing information related to online searches of animal enterprises, their location, owners, information about the city in which they are located, travel routes, restaurants near their route of travel or destination, pictures and videos of animal enterprises, and texts and voicemails related to planned or executed direct actions;
3. Literature **pertaining to** mink, bobcats, and animal rights;
4. Literature **pertaining to** businesses or entities in the meat or animal industry **including but not limited to**: meat plants, meat wholesalers, furriers, and

animal farmers;
12. Maps **of any State, city, county, or location** within the United States;
15. Mailing instruments **including but not limited to**: boxes, labels, postage, envelopes, addresses;
16. Items **thought to** contain blood or DNA of either subject
17. Items **thought to** contain DNA of animals including but not limited to: fur, hair, blood, and fluids;
18. Information pertaining to financial transactions from July 1, 2013, to present; [and]
19. Unopened items **believed to be** destined for resale on Amazon or eBay **including but not limited to**: medications, headlamps, bicycle odometers, electric toothbrush heads, paints, and paint brushes[.]

Exhibit A, p. 16 (emphasis added).

b. The December Warrant

Similarly, the search warrant application for the home and car provides that the items to be sized are: "Items and records constituting and containing evidence, fruits, and /or instrumentalities of violations of 18 U.S.C. §43…." Exhibit B, p. 3. The items to be seized include, "**but not limited to**" the following items:

1. **Any evidence, in any format, related to or used to** commit or facilitate the commission of 18 U.S.C. § 43[;]
2. Digital or paper evidence containing information related to online searches of animal enterprises, their location, owners, information about the city in which they are located, travel routes, restaurants near their route of travel or destination, pictures and videos of animal enterprises; emails, texts, voicemails, pictures, and videos related to planned or executed direct actions; emails, texts, voicemails, pictures, and videos **which would help provide further information about** the conspiracy and crimes committed between July and November 2013[;]
3. Evidence **related to** the vandalism of Mink farms, including maps, trace evidence, breeding cards, receipts, travel documents, photographs, etc.;
4. **Literature pertaining to** mink, bobcats, and animal rights, **including, but not limited to**[:] The Blueprint, Fur Farm Intelligence Project[;] The Full Report; The Final Nail: Destroying the Fur Industry; and Strong Hearts[;]
5. **Literature pertaining to** businesses or entities in the meat or animal industry **including but not limited to**: meat plants, meat wholesalers, furriers, and animal farmers;
6. **Literature and other evidence** indicating motive, including books, articles,

emails, etc., related to direct actions propagated in furtherance of animal rights[;]

17. **Maps of any State, city, county, or location within the United States**;
20. Mailing instruments **including but not limited to**: boxes, labels, postage, envelopes, addresses;
21. Items **thought to contain** blood or DNA of either subject listed in the affidavit;
22. Items **thought to contain** DNA of animals including but not limited to: fur, hair, blood, and fluids;
23. Information **pertaining to** financial transactions from July 1, 2013, to present;
24. Unopened **items believed to be destined for resale** on Amazon or eBay **including but not limited to**: medications, headlamps, bicycle odometers, electric toothbrush heads, new books, new coats, paints, and paint brushes;
28. Evidence, **in any form which would tend to reveal the identities of co-conspirators** and document communication between co-conspirators.

Exhibit B, pp. 3-4 (emphasis added).

c. The Search Warrants Are Overbroad

The seizing authority in the above search warrants is so broad as to allow the seizure on nearly every item found in a car or the house. For instance, item 1 in Exhibit A allows for the seizure of "[a]ny computer systems, digital or analog videos, iPhones and other smartphones, iPods, other digital media storage and playback devices, and cell phones…." Exhibit A, p. 16; *see also* Exhibit B, p. 3 (list items 1 and 2). The government receives the authority to seize all of these devices even though there is no indication that any digital devices were used to commit or facilitate the alleged offenses.

Moreover, many of the items include the following language: **including but not limited to**. *See i.e.*, Exhibit A (items 4, 15, 19); Exhibit B (items 4. 5, 20, 24). The Ninth Circuit rejected identical language in *United States v. Bridges*, 344 F.3d 1010, 1017-18 (9th Cir. 2003). There, the warrant authorized the seizure of records relating to clients or victims, "'including **but not limited to**' the ones listed on the warrant." *Id.* at 1017 (emphasis in opinion). The *Bridges* Court explained: "The wording of this warrant is unquestionably broad in terms of describing what items the federal agents are being asked

to seize. . . .If . . . the scope of the warrant is 'not limited to' the specific records listed on the warrant, it is unclear what is its precise scope or what exactly it is that the agents are expected to be looking for during the search." *Id.* at 1017–18. Such wording violated the Fourth Amendment. *See id.*

Additionally, both warrants give far too much discretion to the seizing agents. The list of items to be seized is replete with references to items **thought** or **believed** to be relevant. *See i.e.,* Exhibit A, p. 16 (items 16, 17, & 19); Exhibit B, p. 3 (items 21, 22, & 24). That violates Ms. Kissane's Fourth Amendment rights because "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir.1982) (citation omitted).

The overbreadth of the warrants is exemplified by the warrant returns. *See* Exhibit O (Evidence Recovery Log from the Car) and Exhibit P (Evidence Recovery Log from the Home). Items seized from the home include nine references to documents; sixteen digital devices; and a "Comb with Red Substance." Exhibit P. In short, the above warrants are fatally overbroad and therefore violate the Fourth Amendment.

2. The Warrants Impermissibly Infringes on Ms. Kissane's First Amendment Rights

The search warrants allow the government to seize "literature pertaining to … animal rights," (Exhibit A, p. 16 (Item 4) and Exhibit B, p. 3 (Item 4)). Additionally, the search warrant for the phone includes the seizure of "[l]iterature and other evidence indicating motive, including books, articles, emails, etc., related to direct actions propagated in furtherance of animal rights." Exhibit B, p. 3 (Item 6).

> The use by government of the power of search and seizure as an adjunct to a system for the suppression of objectionable publications is not new. Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power.

Marchs v. Search Warrants of Property at 104 East Tenth St., 367 U.S. 717, 724 (1961). The use of general warrants to seize publications the government deems inappropriate is "of course, part of the intellectual matrix within which our own constitutional fabric was

shaped." *Id.* at 729. Here, the government's use of such an overbroad warrant to seize all literature pertaining to animal rights is so overbroad that offends Ms. Kissane's First Amendment, Fourth Amendment and Fifth Amendment rights, that the seizure of these items should be suppressed.

3. Suppression is the Appropriate Remedy for an Overbroad Search Warrant

The remedy for an overbroad search warrant is the suppression of the seized evidence. *United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994); *see also United States v. Stubbs*, 873 F.2d 210 (9th Cir. 1989). The government cannot rely on the "good faith" exception to justify the unconstitutional searches. *See United States v. Leon*, 468 U.S. 897, 926 (1984). The Ninth Circuit has cautioned courts to be "vigilant in scrutinizing officers' good faith reliance on . . . illegally overbroad warrants." *United States v. Kow*, 58 F.3d 423, 428 (9th Cir. 1995) (internal quotations omitted). When a warrant lists "broad classes of documents without specific description of the items to be seized," and contains no date-based restriction on those items, "the warrant [is] overbroad [such] that agents could not reasonably rely on it." *Id.* (internal quotations omitted); *see also Weber*, 915 F.2d at 1289 (the government could not rely on the good faith exception because, "at the time [the agent] applied for the warrant, the law was clear that a warrant could not be broader than the probable cause on which it was based."). That is the situation here. Therefore, this court should suppress all evidence seized and derived from the overbroad November and December searches.

C. Delayed Notice is Unconstitutional

An additional reason to suppress evidence from the November 20, 2013 search of the car is that the government did not provide Ms. Kissane with prompt notice that a search warrant was executed. Providing a person notice that their personal property has been searched and or seized is required under both the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure. Since the Fourth Amendment's ultimate touchstone is reasonableness, *Brigham City, Utah v. Stuart*, 547 U.S. 398, 398 (2006), the question is

whether it reasonable to not give notice to a trespassed person for a period exceeding seven days. The answer is no.

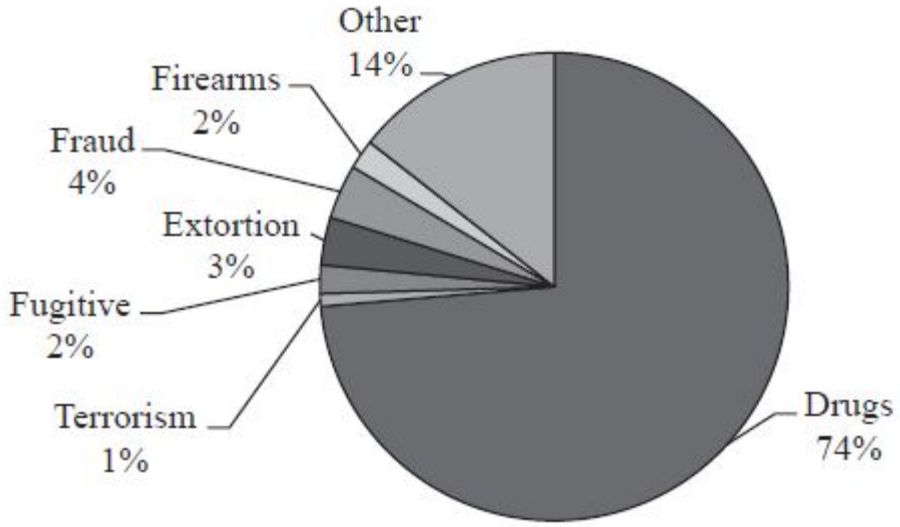
Here, the government sought to delay notification, pursuant to 18 U.S.C. § 3103a, by simply stating: "Because this investigation is continuing, disclosure of this affidavit, the warrant, and/or this application and the attachments thereto will jeopardize the progress of the investigation and will likely cause the subjects of the investigation to change their patterns and destroy evidence as a result of being aware they are under suspicion by the FBI." Exhibit A, p. 11. Failing to provide prompt notice of the search violates the Fourth Amendment.2

Section 3101a provides for what are termed "sneak and steal" or "sneak and peek" warrants. Under this provision, the notice of the execution of a search warrant may be delayed, as relevant here, if "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" and "the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." *Id.* at (b)(1) & (3). Although sneak and peek warrants were codified in the Patriot Act as a method of combating foreign terrorism, they are generally used in drug cases. *See* Jonathan Witmer-Rich, *The Rapid Rise and Delayed Notice of Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 Pepperdine L. Rev. 3 (2014).

---

2 Notice is also addressed by Federal Rules of Criminal Procedure 41(f)(1)(C), which provides that "[t]he officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property"). After Section's 3103a promulgation, Rule 41(f)(3) was added to address delayed notices.

Fig. 3: Federal Delayed Notice Search Warrants, by Case Type, FY 2010



Id. at p. 536.

The Ninth Circuit has not addressed the constitutionality of sneak and steal or sneak and peek warrants after Section 3103a's promulgation. But the Ninth Circuit has addressed the constitutionality of delayed notice warrants. In *United States v. Freitas*, 800 F.2d 1451, 1453 (9th Cir. 1993), the government received a warrant that permitted the agents "to enter the home while no one else was there, look around, and leave without removing anything." The warrant did not include a notice requirement. *Id.* The *Freitas* court addressed, in part, the legality of a warrant that provides no notice requirement. *Id.* at 1455. Ultimately, the court held: "in this case the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing of necessity." *Id.*

This court should find that the failure to provide Ms. Kissane notice within seven days of the search and seizure of her personal property violated her rights under both the Fourth Amendment and the Federal Rule of Criminal Procedure 41. Alternatively, this

court can find that the government did not make a sufficient showing for a delayed warrant by simply concluding: providing prompt notice "will jeopardize the progress of the investigation and will likely cause the subjects of the investigation to change their patterns and destroy evidence as a result of being aware they are under suspicion by the FBI." Exhibit A, p. 11. Regardless of this court's approach, Ms. Kissane moves it to suppress all evidence from the search of her car based on the government's failure to provide prompt notice of the search and seizure of the items from her car.

III. The Search and Seizure of Electronic Data Violated Ms. Kissane's Fourth Amendment Rights.

During the execution of the December warrant, federal agents seized 16 digital devices. There are multiple problems with the search and seizure of these devices and the data they contain. First, the warrant does not establish that there is probable cause to that any of the sixteen digital devices will contain contraband or other seizable evidence. Second, the warrant violates the particularity requirement and fails to include a constitutionally sufficient search methodology. Third, the warrant is unconstitutionally overbroad. Fourth, the warrant fails to include a constitutionally sufficient search methodology. Fifth, the warrant fails to provide for a method for segregating data.

A. The Warrant Lacks Probable Cause To Seize and Search Sixteen Digital Devices

Probable cause for a search requires a "fair probability that contraband or evidence of a crime will be found in a particular place," *Gates*, 462 U.S. at 238, and "probable cause must exist to seize all the items of a particular type described in the warrant." *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d at 857 (citations omitted). Here, the search warrant contains no probable cause that fruits of the alleged offense would be found on any of the sixteen digital devices. That's important because ninety-two percent of Americans own a cell phone.[3] These users are generating a lot of data. In 2014, American cell phone users generated 2.455 trillion minutes of calls and 1.92 trillion text

[3] http://www.pewinternet.org/data-trend/mobile/device-ownership/ (last visited June 26, 2016).

messages. *Id.* The amount of data being consumed has increased significantly over the years. But cell phones are no longer used for just making calls and sending text messages: they are televisions, personal computers, and music players. People use their cell phone to browse the internet more than any other device—an average of 2.8 hour per day.4 A 16 gigabyte cell phone holds the equivalent of 1,200,000 pages of information. That's 600 banker boxes. That's the reason the FBI wanted to search Ms. Kissane's digital devices; they assumed that somewhere in all that data they'd find incriminating evidence. But the Fourth Amendment requires more. The fact that someone who is accused of committing a crime also possesses a digital device does not establish probable cause to search. Here, the search warrant fails to establish probable cause to seize and search the sixteen digital devices.

B. The Warrants Fail To Establish What Data Can Be Searched and Seized

In addition to lacking probable cause, the search warrant violates the particularity requirement, which requires: "'the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize.' 'The description must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized.'" *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009) (citation omitted). "The particularity rule requires the magistrate to make sure that the warrant describes things with reasonable precision, since vague language can cause the officer performing the search to seize objects 'on the mistaken assumption that they fall within the magistrate's authorization.'" *United States v. Weber*, 915 F.2d 1282, 1285 (9th Cir. 1990).

As for the electronic data, the warrant allows the government to seize all digital devices, seize and retain all of the data, and to search all of the content. The warrants

---

4 http://www.smartinsights.com/internet-marketing-statistics/insights-from-kpcb-us-and-global-internet-trends-2015-report/attachment/mobile-internet-trends-mary-meeker-2015-1/ (last visited June 26, 2016).

should have specified whether they were seeking active or deleted data, the type of data (e.g., emails, word documents, photographs, internet searches, cookies, etc.); the location of the data (i.e., allocated, unallocated, cache, etc.). The failure to reasonably identify the data results in the search warrant violating the Fourth Amendment.

C. The Search Warrant Allows For the Overbroad Seizure and Search of Electronic Data

The search warrant authorized a broad, "general, exploratory rummaging" of all the data on the sixteen digital devices seized by the government. *See Weber*, 915 F.2d at 1285 There is no limitation as to the date range of the data being sought. No limitation as to the type of data. And no limitation as to the owner of the device. This is the essence of overbreadth.

The failure to contain an explicit limitation on the age of the data searched is particularly problematic. The warrant allows the seizing and searching of data that is entirely temporally divorced from this case. For instance, if an agent believed he or she needed to search a year-old Facebook message or email to find information "which would help provide further information about the conspiracy and crimes committed between July and November 2013," the warrant lets them do so. Exhibit B, p. 3. Surely, the probable cause, if any, does not extend so far into the past. As the Ninth Circuit explained in *Weber*, "probable cause to believe that some incriminating evidence will be present at a particular place does not necessarily mean there is probable cause to believe that there will be more of the same." 915 F.2d at 1287.

D. The Warrant Fails To Include Constitutionally Sufficient Search Mythology

Search methodologies are critical when staying true to the Fourth Amendment whilst searching electronic data. Magistrate Judge Waxse best described the issue in *In re Search of Premises Known As: A NEXTEL Cellular Telephone*, 14mj8005-DJW, 2014 U.S. Dist. LEXIS 88215 (D. Ks. June 26, 2014). There, considering a similar warrant application, the court explained, "[i]t is true that, in one sense, the government describes a place to be searched—a 'cellular telephone, its computer software, and/or memory storage devices.'

Certainly, this describes the actual thing to be searched. But, an electronic search is not as simple." *Id.* at *37.

In the context of electronic data, the court noted, "a request to search must be accompanied by 'sufficiently specific guidelines for identifying the documents sought ... and [those guidelines must be] followed by the officers conducting the search.' This is precisely what a search protocol is." *Id.* Such a protocol must "explain, with particularity, [the government's] 'methodology for determining, once it is engaged in the search, how it will determine which [storage areas] should be searched for data within the scope of the warrant.'" *Id.*

Turning to the warrant application before it, the court found it "does nothing of the sort. On its face, the Methodology, describes **nothing** with particularity." *Id.* (emphasis in original). According to the court, "[t]he lack of detail is glaring and the explanation tells the Court nothing about how the government intends determine what data falls into the list of items to be seized and what data does not. 'The government should not . . . shy away from explaining what kinds of third party software are used and how they are used to search for particular types of data." *Id.* at * 39. Additionally, "the government does not even explain whether or not its procedures are 'computer assisted' . . . . Moreover, the Methodology does not indicate at what point, if any . . . computer-assisted procedures give way to human inspection." *Id.*

In addition to these concerns, more troubling was the government's failure to "include . . . limitation language. This is an important omission because, as written, the government is requesting it be allowed to search everywhere and seize anything regardless of whether or not the data contained therein falls under the scope of its warrant." *Id.* at *40-41. The court concluded, "the present Methodology does not provide this Court with any meaningful description of the scope of the search it is requesting be authorized." *Id.* at *42. Thus, the warrant application failed to meet the particularity requirement. *See id.* at *36

The same is true in this case. The warrant application contains no protocol or methodology for searching the data. Yet, the search of the home contains a two page

"Protocol For Searching Devices Or Media That Store Data Electronically." Exhibit A, pp. 19-20. The government clearly understood the significance of having search protocols, but simply decided not to include one for the search that resulted in the seizure of 16 digital devices. Thus, this situation here is more egregious than the one presented in *NEXTEL*. This is a fatal flaw. As Judge Hayes has explained, "[t]he search protocol employed must be reasonably directed to identify data within the scope of the warrant in order to meet the particularity requirement. Without this requirement, the search of the electronic data becomes 'general exploratory rummaging in a person's belongings.'" *United States v. Bonner*, No. 12CR3429 WQH, 2013 WL 3829404 at *19 (S.D. Cal. July 23, 2013) reconsideration denied, No. 12CR3429 WQH, 2013 WL 6028301 (S.D. Cal. Nov. 13, 2013). Accordingly, based on the myriad shortfalls in the descriptions of the items to be searched – and lack of meaningful search protocols – the Court should find that the warrants did not satisfy the Fourth Amendment's particularity requirement.

E. The Warrant Provides No Method for Segregating Data

In addition to the lack of a meaningful methodology, the search warrant fails to provide for the segregation of non-reviewable data – *i.e.*, data for which there was no probable cause to search, such as photos and communications with family. Judge Waxse's decision is again illustrative. As to the warrant application before him, he explained that it "d[id] limit the data it seeks to seize, and connects that data to the crimes being investigated—'contact lists, calendars, stored image and video files, internet history, SMS and MMS text messaging, and other data' related to 'drug sales, cultivation, and distribution.'" *NEXTEL*, 2014 U.S. Dist. LEXIS 88215 at *32. But this was insufficient because "the Methodology does not provide the Court with any guidance on how the government intends to determine what data has a nexus to the suspected crime and what data does not." *Id*.

Judge Waxse continued, "[t]o begin with, the government does not indicate whether it will be imaging the device . . . . this Court agrees that 'if the device will be imaged, then there will be a complete copy of all its data--including the data for which there is no probable cause

to seize--that must be accounted for and which ultimately must be purged of data outside the scope of the warrant.'" *Id*. at *32–33. The government's "failure to clarify this point cannot allay this Court's fears that it is authorizing an unlawful search in which the government lacks probable cause to search or seize the data." *Id*. at *33. Judge Waxse held, "[u]ltimately, th[is] omission alone is fatal[.]" *Id*.

However, he was also troubled by the fact that, "[a]lthough the [warrant application's] language implies [] the government will return to the individual all data outside the scope of the warrant, the government does not expressly indicate such an action." *Id.* at 34. And the "Court cannot accept the government's compliance with the Fourth Amendment by implication."

Judge Waxse analogized the government's approach was "to saying that the government will search a residence by looking in all the rooms of the house and opening any desk drawers and cabinets to see what's inside, even though the government is looking for a stolen lawnmower." *Id.* at 41. In other words, "'[j]ust as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom,' probable cause to believe drug trafficking communication may be found in phone's the mail application will not support the search of the phone's Angry Birds application." *Id.* Ultimately, he concluded, "[t]he Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than at a residence." *Id*. at *41-42.

All of the problems Judge Waxse identified were present in the warrant here:

- Nowhere does the government provide any guidance on how it intends to determine what data has a nexus to the suspected crime and what data did not. This runs contrary to the Ninth Circuit's rule that, if "all items in a set of files [are] inspected during a search," there must be "sufficiently specific guidelines for identifying the documents sought [that] are provided in the search warrant and are followed by the officers conducting the search." *United States v. Tamura*, 694 F.2d 591, 594 (9th Cir. 1982).

- The government does not indicate whether it will extract all the data, including the data for which there is no probable cause to seize.

- The government does not provide a means to account for data it seized for which it has no probable cause. It does not direct how it will segregate, return, or destroy that information.

- There is no limitation on the type of files that the government can seize or search.

Any one of these deficiencies should decide the issue in Ms. Kissane's favor. Taken together, they paint an unmistakable picture of an overbroad warrant.

As the Ninth Circuit held in *Bridges*: "[s]earch warrants, including this one, are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet of personal papers and property to be seized at the discretion of the State." *Bridges*, 344 F.3d at 1016. That's the situation present here.

F. Suppression of All Electronic Data

This court should suppress all data seized or derived from the search of the digital devices seized from the search of Ms. Kissane's home. *See* Exhibit B. The suppression of the data is warranted based on any of the above factors, including the lack of probable cause and overbreadth of the warrant.

IV. Suppress Evidence From Section 2703 Orders

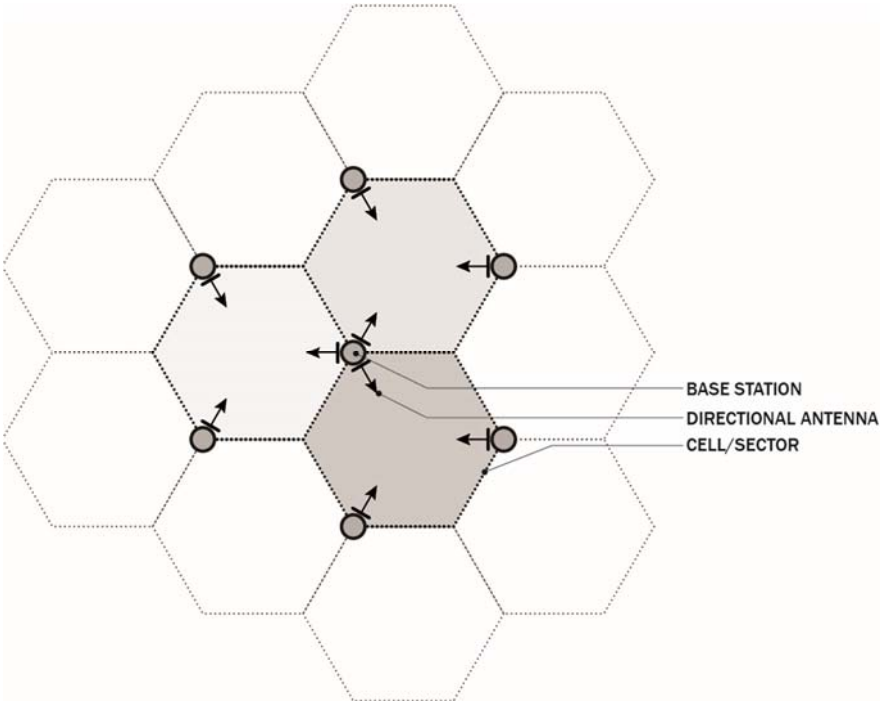
On two occasions, the government received historic cell site data from service providers without the use of a warrant. *See* Exhibits J and K. Instead of requesting the data with a traditional warrant—that is one subject to Federal Rule of Criminal Procedure 41—the government filed an application seeking the records under 18 U.S.C. § 2703. Because the seizure of historic cell site location data implicates a persons' Fourth Amendment rights, the use of a 2703 Subpoena is inappropriate.

A. Technical Background

Cell phones operate through the use of radio waves. Cellular service providers maintain a network of radio base stations (also called cell sites or cell towers) throughout

their coverage areas. *See* Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong., 50 (2013) (written testimony of Prof. Matt Blaze, University of Pennsylvania) [hereinafter 2013 ECPA Hearing]. A base station consists of multiple antennas facing in different directions. Typically, there are three antennas, each covering a 120-degree arc, resulting in three pie-shaped sectors. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Att'y Bull., Nov. 2011, at 19-20 [hereinafter O'Malley].

Cell phones periodically identify themselves to the closest base station (the one with the strongest radio signal) as they move throughout the coverage area. *See* 2013 ECPA Hearing at 50. Whenever a cell phone user makes or receives a call or text message, his phone connects, via radio waves, to an antenna on a cell site, generating cell site location information ["CSLI"]. If a cell phone moves away from the base station with which it started a call and closer to another base station, it connects seamlessly to the next base station. *Id.*



As the number of cell phones has increased, the number of cell sites has had to increase as well:

> A sector can handle only a limited number of simultaneous call connections given the amount of radio spectrum "bandwidth" allocated to the wireless carrier. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and

> antenna. New services, such as 3G and LTE/4G Internet create additional pressure on the available spectrum bandwidth, usually requiring, again, that the area covered by each sector be made smaller and smaller.

Id. at 54. Densely populated urban areas therefore have more towers covering smaller sectors.

The trend is toward smaller and smaller base stations – called microcells, picocells, or femtocells – that cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home. *Id.* at 43-44. The effect of this proliferation of base stations is that "knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area … sometimes effectively identifying individual floors and rooms within buildings." *Id.* at 55-56. Although the ability of cell providers to track a phone's location within a sector varies based on a number of factors, it is increasingly possible to use CSLI to "calculate users' locations with a precision that approaches that of GPS." *Id.* at 53.

Tools and techniques are continually being developed to track CSLI with ever-greater precision. Providers currently can triangulate the location of a phone within a sector by correlating the time and angle at which it connects with multiple base stations. *Id.* at 56. Providers are also developing technologies that will track CSLI whenever a phone is turned on, whether or not it is in use. *Id.* at 57. Because this information costs little to collect and store, providers tend to keep it indefinitely. *See* Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services, Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., 16 (2010) (testimony of Prof. Matt Blaze) [hereinafter 2010 ECPA Hearing].

The ability to track people through their cell phones is, obviously, very appealing to law enforcement. *See* O'Malley, *supra*, at 26 (noting that provider records "contain accurate date, time, and location information" and "unlike a witness' memory, are not prone to impeachment based on their accuracy, reliability, or bias"); 2013 ECPA Hearing

at 61 ("These characteristics – ubiquitous and continuous availability, lack of alerting, and high precision – make network-based cellular tracking an extremely attractive and powerful tool for law enforcement surveillance.").

Consequently, each year, the United States government seeks CSLI for tens of thousands of people. *See* 2010 ECPA Hearing at 80 (written testimony of United States Magistrate Judge Stephen Wm. Smith). The government almost always seeks this information by way of sealed applications and orders. *Id.* at 87.

B. Section 2703(d) Applications and Orders

The government obtained CSLI through use of court orders issued under the Stored Communications Act ["SCA"], 18 U.S.C. § 2703(d), directing AT&T, Sprint, T-Mobile, and Verizon Wireless to disclose the information. *See* Exhibit J, p. 1; Exhibit K, p.1. With respect to the July 18, 2013 subpoena, the government sought to obtain records: "identifying any wireless telephone call (including the phone numbers and subscriber information of the sending and receiving phones) originating, terminating, or conducted through cell sites providing coverage to 7670 Clairemont Mesa Boulevard San Diego CA 92117, 3674 Birdie Drive, La Mesa CA 91941, and 9589 Upland Street Spring Valley, CA 91777, from 8:00 p.m. on July 14 2013 through 8:00 a.m. on July 15, 2013." Exhibit J, p. [5] 2. With respect to the April 29, 2014 Application, the government sought to obtain records: "identifying any wireless telephone call (including the phone numbers and subscriber information of the sending and receiving phones) originating, terminating, or conducted through cell sites providing coverage to 33327 Terrace Lake Road, Ronan, Montana, from 8:00 PM MST on 03/06/2014 through 8:00 AM MST 03/07/2014." Exhibit K, p. 2. These applications, although filed under the SCA, violate the Fourth Amendment.

---

5 To put this request in context, within a four mile radius of 7670 Clairemont Mesa Boulevard, there are 260 towers and 544 antennas. *See* http://www.antennasearch.com/sitestart.asp (last visited July 15, 2016) (providing information regarding the concentration of towers in a given geographic area).

The SCA "provid[es] an avenue for law enforcement entities to compel a provider of electronic communication services to disclose the contents and records of electronic communications." *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 287 (4th Cir. 2013) (hereinafter "*In re Application*"); *see also* 18 U.S.C. §§ 2701–2711 (2010). The statute outlines procedures a governmental entity must follow to procure information from a service provider, treating subscriber account records differently than the content of electronic communications. *United States v. Clenney*, 631 F.3d 658, 666 (4th Cir.2011) (*citing* 18 U.S.C. § 2703).

Absent subscriber notice and consent, the government must secure a warrant or a court order for subscription account records. 18 U.S.C. § 2703(c)(1). A warrant from a federal district court for the disclosure of subscriber records must be issued pursuant to the Federal Rules of Criminal Procedure, *id.* § 2703(c)(1)(A), which, in accordance with the Fourth Amendment, require a finding of probable cause by an impartial magistrate. *See* Fed.R.Crim.P. 41(d); *see also Payton v. New York*, 445 U.S. 573, 588 n. 26 (1980). Section 2703(d) sets out the requirements for a court order for a service provider to disclose subscriber account records. The government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). "This is essentially a reasonable suspicion standard[,]"*In re Application*, 707 F.3d at 287, in contrast to the substantially higher probable cause standard for securing a warrant. The statute offers no express direction as to when the government should seek a warrant versus a § 2703(d) order.

C. 2703 Applications Violate the Fourth Amendment

The Fourth Amendment prohibits the government from collecting an individual's historical location tracking information without a warrant. Since at least 1967, the Supreme Court has recognized that the Fourth Amendment protects an individual's right to privacy, even in public places. *Katz v. United States*, 389 U.S. 347, 351 (1967). *Katz* held that when the government infringes upon a subjective expectation of privacy that

society recognizes as reasonable, it effects a search and seizure within the meaning of the Fourth Amendment. *Id.* at 353. Thus, in *Katz*, the government was found to have violated the defendant's Fourth Amendment rights by eavesdropping on his private conversation in a public phone booth. *Id.*

In *United States v. Knotts*, the Court first applied the *Katz* test to electronic surveillance, holding that the Fourth Amendment was not violated when the government used a beeper to track a car. 460 U.S. 276, 277 (1983). The beeper tracking in *Knotts* did not implicate the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. However, the Court left open the possibility that advances in surveillance technology would require it to reevaluate its decision. *Id.* at 283-84.

The following year, in *United States v. Karo*, the Court limited *Knotts* to electronic surveillance in public places. 468 U.S. 705, 714 (1984). In *Karo*, the police placed a beeper in a container belonging to the defendant and monitored its location electronically, including while it was inside a private residence. *Id.* at 708-10. The Court held that the monitoring of the beeper inside the home was an unconstitutional trespass into the residence by electronic means – even though the officers could not have known, when they planted the tracking device that it would end up inside a house. *Id.* at 715; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that the government engages in a search in violation of the Fourth Amendment by using a thermal imager to detect heat signatures inside a house that would be invisible to the naked eye).

More recently, in *United States v. Jones*, five Justices concluded that prolonged electronic location monitoring by the government, even when it is limited to public locations, impinges upon a legitimate expectation of privacy in violation of the Fourth Amendment. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 965 (Alito, J., concurring). In *Jones*, the government placed a GPS tracker on the defendant's car and used it to monitor the car's location – on public thoroughfares – for 28 days. *Id.* at 948.

The majority opinion held that the government had violated the Fourth Amendment by the physical trespass of placing the tracker on the vehicle, and it therefore did not need to address whether the location tracking violated a reasonable expectation of privacy. *Id.* at 949. It explicitly noted, however, that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis." *Id.* at 953.

The five Justices who did engage in a *Katz* analysis concluded that the government's actions in tracking the car's location violated the Fourth Amendment. *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).[6] Although the government tracked the car only as it travelled in plain sight on public streets and highways, Justice Alito concluded that the GPS monitoring "involved a degree of intrusion that a reasonable person would not have anticipated." *Id.* at 964 (Alito, J., concurring). Consequently, he found that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* Notably, this conclusion did not depend upon on the type of technology used to track the car in *Jones*; rather, Justice Alito discussed the proliferation of modern devices that track people's movements, noting that cell phones were "perhaps [the] most significant" among these. *Id.* at 963 (Alito, J., concurring).

Justice Sotomayor agreed that prolonged electronic surveillance violates the Fourth Amendment. *Id.* at 955 (Sotomayor, J., concurring). She added, however, that "even short-term monitoring" raises concerns under *Katz* because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* When governmental actions intrude upon someone's privacy to that degree, a warrant is required. *Id.*

---

6 Justice Sotomayor, while agreeing with Justices Alito, Ginsburg, Breyer, and Kagan that an analysis under *Katz* was appropriate, nonetheless wrote separately because she also joined the majority in concluding that the physical trespass of placing the tracker on the car was an independent Fourth Amendment violation. *Jones*, 132 S. Ct. at 954-55 (Sotomayor, J., concurring).

The data the government seeks when it requests CSLI is much more comprehensive, and much more apt to reveal intimate information, than the location of someone's car. Indeed, although people are in their cars only while travelling from one place to another, most Americans are within five feet of their cell phones most of the time.[7] Especially in urban settings, where cell towers are more plentiful, a cell phone – and, by extension, its owner – can be tracked with disquieting precision.[8]

Several courts have recently held that CSLI implicates the Fourth Amendment and therefore requires a warrant. In *In re: Application For Telephone Information Needed For a Criminal Investigation*, 15xr90304-HRL-1(LHK) (N.D. Cal. July 29, 2015), District Court Judge Lucy H. Koh held:

> cell phone users have an expectation of privacy in the historical CSLI associated with their cell phones, and that society is prepared to recognize that expectation as objectively reasonable. Cell phone users do not expect that law enforcement will be able to track their movements 24/7 for a sixty-day period simply because the users keep their cell phones turned on. That expectation, the Court finds, is eminently reasonable.

Id. at p. 22 (attached as Exhibit Q). The Court reached this conclusion, in part, after recognizing that:

> (1) an individual's expectation of privacy is at its pinnacle when government surveillance intrudes on the home;
> (2) long-term electronic surveillance by the government implicates an individual's expectation of privacy; and

---

7 Harris Interactive, *2013 Mobile Consumer Habits Study*, Jumio, Inc., 2 (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20%20Mobile%20Consumer%20Habits%20Study-2.pdf (last viewed Aug. 20, 2015).

8 Even cases that disagree on the constitutionality of warrantless CSLI tracking acknowledge that the tracking is precise. *See In the Matter of the Application*, 724 F.3d 600, 609 (5th Cir. 2013) ("The reason that the Government seeks such information is to locate or track a suspect in a criminal investigation. The data must be precise enough to be useful to the government… it can narrow someone's location to a fairly small area."); *see also* 2013 ECPA Hearing at 61 ("The increasingly high resolution that the cell site tracking can achieve in densely populated areas – and the ability to provide this data even when the handset is indoors – can paint an even richer picture of an individual's movements than can vehicle-based GPS devices.").

> (3) location data generated by cell phones, which are ubiquitous in this day and age, can reveal a wealth of private information about an individual.

Id. at 16; *see also United States v. Cooper*, 13cr693-SI (N.D. Cal. Mar. 2, 2015) (same).[9]

Here, there is a reasonable expectation of privacy in historic CSLI. By obtaining this information without probable cause and a warrant, the government violated Ms. Kissane's Fourth Amendment rights. Accordingly, this Court should suppress all cell site information and other evidence obtained from the Section 2703(d) Order.

V. Evidence From The Search of The Car and House Because The Government Deliberately Included False and Misleading Statements In the Search Warrant Application.

The government may not deliberately make false statements in an application for a search warrant. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). "[T]he Fourth Amendment mandates that a defendant be permitted to challenge a warrant affidavit valid on its face when it contains deliberate or reckless omissions of fact that tend to mislead." *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985). A defendant is entitled to a hearing if he makes a substantial preliminary showing that an affidavit contains deliberate or reckless omissions of fact that tend to mislead. *Id.*

Here, the November 19th application to covertly search Ms. Kissane's car (Exhibit A) and the December 17th application to search Ms. Kissane's car and her mother's home (Exhibit B) both contain the same false statement: "The FBI's ongoing investigation of Kissane and Buddenberg and analysis of travel, statements provided to law enforcement, **and interviews with Kissane's relatives indicate that Kissane and Buddenberg traveled interstate to damage and/or interfere with various animal enterprises in violation of 18 U.S.C. § 43.**" Exhibit A, p. 3; Exhibit B, p. 3 (emphasis added). In other words, this sentence suggest that Ms. Kissane's relatives confirmed that she was traveling across the country to damage and interfere with various animal enterprises.

---

9 Other court, including *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir.2013), and the *en banc* Eleventh Circuit in *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015), have reached the opposite conclusion.

That's significant because, save for reference to the family, the government's entire theory of probable cause is based on circumstantial evidence. But this statement is false.

To prevail on a claim that the police procured a warrant through deception, the party challenging the warrant must show that the affiant deliberately or recklessly made false statements or omissions that were material to the finding of probable cause. *See Ewing v. City of Stockton*, 588 F.3d 1218, 1223 (9th Cir.2009).

None of Ms. Kissane's relatives indicated that Ms. Kissane was traveling across the country in order to damage or interfere with animal enterprises. And the agents who wrote the applications were the same agents who interviewed Ms. Kissane's family members. Agent Deborah Frye, who wrote the application to search Ms. Kissane's car (Exhibit A) and Agent Justin Menolascino, who wrote the application to search the home and car (Exhibit B) interviewed Ms. Kissane's mother Cathy (Exhibit M) and Ms. Kissane's aunt Kerrie (Exhibit N). Neither relative confirms that the purpose of Ms. Kissane's cross-country travel was to damage and interfere with various animal enterprises. The reason that Agent Frye and Agent Menolascinio included these false statements in their search warrant applications was because without them, the statements lacked probable cause.

Next, after finding the statements were deliberately (or recklessly included), this court must evaluate the materiality of the statements, which requires: "the court [to] purge[] those statements and determines whether what is left justifies issuance of the warrant." *City of Stockton*, 588 F.3d at 1224. "If probable cause remains after amendment, then no constitutional error has occurred." *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1084 (9th Cir.2011). Here, if the court purges the deliberately misleading statements, then no probable cause exists to search either Mr. Kissane's car or the home of her mother. Accordingly, Ms. Kissane moves this Court to suppress the evidence seized and derived during the search of her car and her mother's house, or alternatively, for a hearing in order to question Agents Frye and Menolascino.

VI. Request For Notice of the Government's Intent to Introduce Evidence and Motion for Leave to File Further Motions

The government has provided the defense with a substantial amount of discovery. At this point, it is unclear if the government has provided to the defense all of the evidence it received from various warrants, subpoenas and applications.10 In order to expedite briefing in this case, Ms. Kissane moves this court to order the government to provide information pursuant to Federal Rule of Criminal Procedure 12(b)(4)(B), which provides: "[a]t the arraignment or as soon afterward as practicable, the defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16." Federal Rule of Criminal Procedure 16 provides, in relevant part, that "[u]pon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant." Fed.R.Crim.P. 16(a)(1)(E). Rule 12(b)(4)(B) is intended to make it possible for defendants to "avoid the necessity of moving to suppress evidence which the government does not intend to use." Fed. R. Crim. P 12 advisory committee's note (1974). Therefore, Ms. Kissane moves this court to order the government to provide notice of evidence it seeks to admit in trial and the ability to file further motions in response.

---

10 For instance, at this point, it is unclear if the government received evidence regarding the applications set forth in Exhibits C, D, E, G, H & I.

VII. Conclusion

For the above reasons, Ms. Kissane moves this Court to suppress the evidence as set forth above.

Respectfully submitted,

DATED: July 19, 2016

/s/ John C. Ellis, Jr.

John C. Ellis, Jr.
Reuben C. Cahn
Federal Defenders of San Diego, Inc.
Attorneys for Ms. Kissane
john_ellis@fd.org
reuben_cahn@fd.org

CERTIFICATE OF SERVICE

Counsel for the Defendant certifies that the foregoing pleading has been electronically served on the following parties by virtue of their registration with the CM/ECF system:

John N. Parmley
Assistant U.S. Attorney

Michael F. Kaplan
Assistant U.S. Attorney

Respectfully submitted,

DATED: July 19, 2016

/s/ John C. Ellis, Jr.

John C. Ellis, Jr.
Reuben C. Cahn
Federal Defenders of San Diego, Inc.
Attorneys for Ms. Kissane
john_ellis@fd.org
reuben_cahn@fd.org